Justin M. Baxter, Oregon State Bar ID Number 992178
Email: justin@baxterlaw.com
BAXTER & BAXTER, LLP
8835 S.W. Canyon Lane, Suite 130
Portland, Oregon 97225
Telephone (503) 297-9031
Facsimile (503) 291-9172

Attorneys for Plaintiffs

IN THE UNITED STATE DISTRICT COURT
FOR THE DISTRICT OF OREGON
PORTLAND DIVISION

RICHARD SMITH, on behalf of himself and all others similarly situated, Plaintiff, v. **KAYE-SMITH ENTERPRISES, INC.**, Defendant.	NO. **CLASS ACTION COMPLAINT** **DEMAND FOR JURY**

Plaintiff Richard Smith, individually and on behalf of all other similarly situated ("Class Members"), brings this Complaint against Defendant Kaye-Smith Enterprises, Inc. ("Kaye-Smith"), and alleges the following based on personal knowledge as to his own actions, based on his counsel's investigations, and upon information and belief as to all other matters as follows:

I. INTRODUCTION

1. Plaintiff brings this action against Kaye-Smith for its failure to protect and properly secure his and other people's sensitive personal and financial information including their names, Social Security numbers, addresses, phone numbers, dates of birth, financial account numbers,

and/or credit scores (collectively "personally identifiable information" or "PII"),[1] and for its failure to timely advise Plaintiff and others that their PII had been compromised.

2. Kaye-Smith, is a vendor that generates monthly account statements for various institutional clients including Boeing Employees' Credit Union ("BECU"). On or before June 6, 2022, Kaye-Smith informed BECU that an unauthorized actor breached Kaye-Smith's computer network, thereby gaining access to the PII of members that BECU had shared with it (the "Data Breach"). Kaye-Smith determined that during the Data Breach, one or more unauthorized actors gained access to the PII of Plaintiff and over 344,000 Class Members, that included, but was not limited to, their names, addresses, account numbers, credit information, and Social Security Numbers. These Class Members have already suffered injury and ascertainable losses in the form of the present and imminent threat of fraud and identity theft, loss of the benefit of their bargain, out of pocket expenses, loss of value of their time incurred to remedy or mitigate the effects of the attack, and the loss of, and diminution in value of their PII.

3. Neither BECU nor Kaye-Smith has revealed exactly when the breach occurred, over how much time it occurred, or whether it involved a single event or had been ongoing. It is clear however, that both BECU and Kaye-Smith waited at least six weeks and possibly significantly longer before notifying the public and before notifying members whose PII may have been compromised. BECU members' PII was, according to BECU, released by an unnamed vendor to whom BECU had given access to the information for the purpose of providing services

[1] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 CFR § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on their face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security number, passport number, driver's license number, financial account number).

for BECU. Kaye-Smith was the vendor to which BECU's notice referred.

4. BECU's members entrust it with an extensive amount of their PII. BECU retains this information on computer hardware and shares this PII with vendors such as Kaye-Smith in the course of outsourcing banking services, as well as marketing services. Both Kaye-Smith and BECU assert that they understand the importance of protecting such information.

5. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, Kaye-Smith assumed legal and equitable duties to those individuals.

6. The exposed PII of Plaintiff and Class Members can be sold on the dark web. Hackers can access and then offer for sale the unencrypted, unredacted PII to criminals. Plaintiff and Class Members face a lifetime risk of identity theft, which is heightened here by the loss of Social Security numbers.

7. This PII was compromised due to Kaye-Smith's negligent and/or careless acts and omissions and their respective failure to protect PII of Plaintiff and Class Members and to maintain adequate safeguards.

8. Plaintiff and Class Members suffered and will continue to suffer injury due to Defendants' conduct. These injuries include: (i) lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, and significantly (iv) the continued and certainly an increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII. Plaintiff and

Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

II. PARTIES

9. Plaintiff was a resident of Pierce County, Washington at times relevant to this action and has recently relocated to Pima County, Arizona.

10. Defendant Kaye-Smith is a for-profit corporation organized under the laws of Oregon, with its principal office located in Renton, Washington and one of three primary offices located in Portland, Oregon.

III. JURISDICTION AND VENUE

11. This Court has subject matter jurisdiction over Plaintiff's claims under 28 U.S.C. § 1332(d)(2), because (a) there are 100 or more Class members, (b) Plaintiff is a citizen of a state that is diverse from Defendant's citizenship, and (c) the matter in controversy exceeds $5,000,000, exclusive of interest and costs.

12. This Court has personal jurisdiction over Defendant because it is organized under the laws of the State of Oregon, maintains an office in this District and does business in Oregon and/or transacted business in Oregon.

13. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(2) because Kaye-Smith's place of business is located in this District.

IV. FACTUAL ALLEGATIONS

Background

14. BECU collected and stored some of Plaintiff's and Class Members' most sensitive and confidential information, including Social Security numbers, home addresses, phone numbers, dates of birth, financial account numbers, and other PII, which is static, does not change, and can be used to commit myriad financial crimes.

15. BECU's members entrust BECU with an extensive amount of their PII. BECU in turn, entrusted Kaye-Smith with this PII.

16. On information and belief, Kaye-Smith contracted with BECU, at in Washington, to provide vendor services to BECU. In the course of providing those services, Kaye-Smith obtained the PII of Plaintiff and Class Members that was transmitted from BECU's servers in King County, Washington. Kaye-Smith retains this information on computer hardware and asserts that it understands the importance of protecting such information.

17. Plaintiff and Class Members relied on this sophisticated Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members demand security to safeguard their PII.

18. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, Kaye-Smith assumed legal and equitable duties to those individuals.

19. Kaye-Smith was aware, or should reasonably have been aware, that the PII it agreed to obtain and safeguard is highly sensitive and of significant value to those who would use it for wrongful purposes.

20. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[2] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's

[2] 17 C.F.R. § 248.201 (2013).

license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[3]

21. PII is a valuable commodity to identity thieves once the information has been compromised. As the FTC recognizes, once identity thieves have PII, "they can drain your bank account, run up your credit cards, open new utility accounts, or get treatment on your medical insurance."

22. Identity thieves can use PII such as the PII of Plaintiff and Class Members which Defendants failed to secure, to perpetrate other varieties of crimes that harm victims. A "cyber black market" exists in which criminals openly post and sell PII. Hackers can access and then offer for sale the unencrypted, unredacted PII to criminals. Plaintiff and Class Members face a lifetime risk of identity theft, which is heightened here by the loss of Social Security numbers.

23. Professionals tasked with combatting cybercriminals know that PII has real monetary value in part because criminals continue their efforts to obtain this data. In other words, if any additional breach of sensitive data did not have incremental value to criminals, a reduction in criminal efforts to obtain such data over time would occur. However, just the opposite has occurred, with data breaches rising

24. This PII was compromised due to Kaye-Smith's negligent and/or careless acts and omissions and the failure to adequately protect PII of Plaintiff and Class Members.

25. Kaye-Smith bills itself as "a leader in the execution and management of business-critical communications." It touts on its website its "three pillars of security" which "allow us to meet and exceed the most stringent requirements associated with data communications, and

[3] *Id*.

materials handling for the financial, medical, biotech and insurance industries." As such, Kaye-Smith is well aware of the need to protect PII.

26. Kaye-Smith assumed a non-delegable duty to protect the PII of Plaintiff and the Class members.

27. Ransomware is a malware designed by cybercriminals to deny a user or organization access to files on their computer. By encrypting these files and demanding a ransom payment for the decryption key, cybercriminals place organizations in a position where paying the ransom is the easiest and cheapest way to regain access to their files. Some variants have added additional functionality – such as data theft – to provide further incentive for ransomware victims to pay the ransom. Ransomware has quickly become the most prominent and visible type of malware. Kaye-Smith and BECU, at all relevant times, knew or should have known that cyber criminals seek out PII, especially through ransomware.

28. Best practices such as cyber awareness training, continuous data backups, patching, and encryption all exist to prevent ransomware attacks by cybercriminals.

The Data Breach

29. On July 29, 2022, Plaintiff received a letter from BECU dated July 25, 2022 entitled "Important Privacy Protection Notification." that stated:

> At BECU, we value your business and respect the privacy of your information, which is why we are writing to let you know about a vendor network security incident that involves your personal information. We encourage you to read this entire letter because it contains important information concerning the security of your account(s) at BECU. It also includes our offer to provide you with one year of credit monitoring protection at no cost to you unless otherwise required by local law. We take the protection of your information very seriously and are contacting you directly to explain the circumstances of the incident. To learn more, visit becu.org/vendor-incident.

What happened?

On June 6, 2022, BECU was informed that its printing vendor had experienced a network security incident. At that time, BECU took immediate measures to protect member information by suspending services with the vendor. After the incident occurred, the vendor indicated that some BECU member information in process at the time of the incident was potentially involved. On July 5, 2022, we were able to determine that your personal information was involved after an independent forensics firm had analyzed the compromised data. We sincerely apologize for any inconvenience or concern this incident may cause.

What information was involved?

The information involved may have included your name, address, account number(s), credit score, and Social Security number.

What we are doing.

The security of accounts and the protection of personal information – for you and all our members – are top priorities at BECU. We are committed to ensuring the security of your personal information. BECU worked with the vendor and a forensics firm before resuming services to improve the security of the vendor's environment as well as its effectiveness at preventing and detecting future cybersecurity incidents.

We understand you may have concerns, so we have secured Equifax Credit Watch™ Gold to provide you credit monitoring protection at no cost for one (1) year unless otherwise required by local law.

30. On July 23, BECU posted a notice on its website, which it updated on July 25.[4]

What Happened

On June 6, BECU was informed that our third-party printing vendor had experienced a network security incident that impacted their printing and notification services for our members and involved unauthorized access to certain data of some members. At that time, BECU took immediate measures to protect member information by suspending services with the vendor.

[4] *See* https://www.becu.org/news/2022/important-notice-about-vendor-incident-and-delayed-statements

The vendor engaged a third-party forensics firm to investigate the incident to identify what data was accessed and to restore operations. We continued to communicate with the vendor regularly throughout the investigation to monitor and understand implications for members.

On July 5, we were able to determine what information was accessed after the third-party forensics firm analyzed the incident and provided their findings. We are satisfied with the steps the vendor has undertaken and have resumed regular operations.

As of July 25, we have begun notifying impacted members with letters sent via USPS mail. As shared in the notification, members with questions or concerns about this incident can reach out to our partner Epiq Corporate Services at 877-390-2571, Monday-Friday, 7 a.m.-7 p.m. Pacific Time. We take the security of our members' accounts and personal information very seriously and sincerely apologize for any inconvenience or concern this incident may cause.

As BECU resumed services with the vendor, members are receiving their delayed statements and correspondence. While all monthly statements will be available by the end of July, we expect that some delivery delays will continue for several weeks as we return to regular production schedules. Members may also have received some statements and correspondence out of order. We recognize the inconvenience and we appreciate your patience while we work to get caught up.

Who Is Affected?

We understand you may have concerns and we take these matters very seriously. We began mailing letters on July 25 to members whose data was impacted by the incident. Members with questions or concerns on this incident can reach out to our partner Epiq Corporate Services at 877-390-2571. We encourage you to refer to the FAQ below for steps to be proactive with your account security.

Our Commitment

Securing and protecting our members' privacy and sensitive information remains our highest priority. We continually monitor accounts for suspicious and unauthorized activity. We are communicating to all members whose data was impacted by the incident and provided an offer for free credit monitoring protection for reassurance and increased security.

When we were informed of the incident, BECU immediately suspended services with the vendor. As a result of this service interruption, delivery of monthly statements and other correspondence to members was delayed. We worked to provide alternative options during this time and

> implemented back-up processes for communication to members, as much as possible. We apologize for any inconvenience you may have experienced.

31. BECU admitted in its website notice and in the letter it sent to Plaintiff and to Class Members that a vendor (later identified as Kaye-Smith) with whom BECU had contracted to provide printing services, allowed unauthorized access to the members' PII that it received from BECU. Kaye-Smith was subject to a ransomware attack that included the PII of Plaintiff and other BECU members as well as the PII of various non-profit contributors and hospital patients/customers.

32. BECU claimed that in response to the Data Breach, it "took immediate measures to protect member information." Yet the only measure it identifies taking was temporarily suspending services with Kaye-Smith. Such measures were ineffectual as the PII had already been released.

33. Though its notice is carefully stated, BECU acknowledges taking little or no remedial action of its own. BECU states that "the vendor engaged a third-party forensics firm to investigate the incident," but the scope of the investigation was only "to identify what data was accessed and to restore operations."

34. Neither Kaye-Smith nor BECU has shared with Plaintiff or with Class Members the root cause of the Data Breach, the vulnerabilities exploited, and what, if any, remedial measures they have undertaken to ensure a breach does not occur again. Plaintiff and Class Members retain a vested interest in ensuring that their information remains protected.

35. Plaintiff and Class Members' unencrypted information may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can easily access the PII of Plaintiff and Class Members.

36. Kaye-Smith did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining for Plaintiff and for Class Members, causing their PII to be exposed.

Kaye-Smith is Entrusted with Plaintiff's and Class Members' PII.

37. BECU acquired, collected, and stored Plaintiff's and Class Members' PII that it collects at the time each member opens an account as a condition of providing services to its customers.

38. BECU contracted with Kaye-Smith to provide vendor services and then entrusted Kaye-Smith the PII of Plaintiff and Class Members. Upon accepting this sensitive information, Kaye-Smith assumed legal and equitable duties and knew or should have known that it was responsible for protecting the PII from disclosure.

39. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and relied on BECU and its vendors, including Kaye-Smith to keep their PII confidential and securely maintained, to use this information for business purposes only, to adequately ensure that any third-party vendors maintained adequate procedures and safeguards to keep the PII BECU provided confidential, and to make only authorized disclosures of this information.

Securing PII and Preventing Breaches.

40. Kaye-Smith could have prevented this Data Breach by properly securing and encrypting the PII of Plaintiff and Class Members.

41. Kaye-Smith's negligence in safeguarding the PII of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

42. Despite the prevalence of public announcements of data breach and data security

compromises, Kaye-Smith failed to take appropriate steps to protect the PII of Plaintiff and Class Members from being compromised.

43. The ramifications of Defendant's failure to keep secure the PII of Plaintiff and Class Members are long lasting and severe. Once PII is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

Value of Personal Identifiable Information

44. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[5] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[6] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[7]

45. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number

---

[5] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed August 1, 2022).

[6] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed August 1, 2022).

[7] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed August 1, 2022).

> and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[8]

46. Changing or canceling a stolen Social Security number is a difficult task. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted because an individual must show evidence of actual, ongoing fraud activity to obtain a new Social Security number.

47. Moreover, a new Social Security number may not be an effective remedy to an identity theft. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[9]

48. Based on the foregoing, the information compromised in Kaye-Smith's Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and it is difficult, if not impossible, to change.

49. This data that Kaye-Smith failed to safeguard demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared

---

[8] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed August 1, 2022).

[9] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last accessed August 1, 2022).

to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[10]

50. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

51. The PII of Plaintiff and Class Members was likely taken by hackers to engage in identity theft or and or to sell it to other criminals who will purchase the PII for that purpose. The fraudulent activity resulting from Kaye-Smith's Data Breach may not come to light for years.

52. There may also be a time lag between when harm occurs versus when it is discovered and also between the time PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[11]

53. At all relevant times, Kaye-Smith knew, or reasonably should have known, the importance of safeguarding Plaintiff's and Class Members' PII and of the foreseeable consequences that would occur if the PII was compromised, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members.

54. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiff and Class Members are

---

[10] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed August 1, 2022).

[11] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/products/gao-07-737 (last accessed August 1, 2022).

incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

55. To date, BECU has offered Plaintiff and Class Members only one year of identity monitoring through a single provider. This is inadequate to protect Plaintiff and Class Members from the threats they face for years to come, particularly in light of the PII at issue here. Kaye-Smith has offered Plaintiff and Class Members nothing.

56. The injuries to Plaintiff and Class Members were directly and proximately caused by Kaye-Smith's failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

Plaintiff Richard Smith's Experience

57. Richard Smith is a retired Kitsap County, Washington Deputy Sheriff.

58. In approximately 2009 Mr. Smith opened both a personal checking account and a business account at a BECU branch in Tacoma, Washington. He had transferred to BECU from Bank of America after becoming disillusioned with what he felt were incessant and unjustified fees Bank of America was charging and wanted to bank at a smaller and more consumer-friendly institution. He was, however, wary of banking at a small credit union that may not have sufficiently sophisticated safeguards to protect his sensitive information. He chose BECU in part, based on BECU's assurances regarding its level of sophistication and its commitment to keeping sensitive information secure—including when sharing information with its vendors.

59. As a condition of opening accounts at BECU, Mr. Smith was required to provide detailed PII that included his address, telephone number, email address, Social Security number, date of birth, business tax identification number, and driver's license number. BECU stored and/or shared some of Mr. Smith's most sensitive (and extremely valuable to cyber criminals and identity thieves) PII resulting in the exposure of Mr. Smith's PII during the Data Breach.

60. After learning of the Data Breach, Mr. Smith purchased a subscription to an identity theft protection service and credit monitoring service.

61. In addition, as a result of learning of the Data Breach, Mr. Smith has spent, and is continuing to spend, time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the news reports of the Data Breach, at least two hours exploring credit monitoring and identity theft insurance options, and self-monitoring his financial accounts. This time has been lost and cannot be recaptured.

62. Mr. Smith has been careful about sharing his PII. He has not knowingly transmitted unencrypted PII over the internet or any other unsecured source, and stores documents containing his PII in a secure location or destroys the documents.

63. Mr. Smith suffered actual injury in the form of money spent on credit monitoring and identity theft protection as well as damages to, and diminution of the value of his PII—a form of intangible property that Mr. Smith entrusted to BECU as a customer, that was in turn entrusted to Defendant, and which was compromised in and as a result of the Data Breach.

64. Mr. Smith has also suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety, distress, and increased concerns for the loss of his privacy.

65. Since the Data Breach, Mr. Smith has received a text message purportedly from BECU in response to someone attempting to change his BECU password. This has caused him further legitimate concern that bad actors are actively attempting to access his BECU account illegitimately.

66. Mr. Smith has suffered additional injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII, especially his Social Security

number, in combination with his name and Social Security number being placed in the hands of unauthorized parties and possibly criminals.

67. Mr. Smith has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

V. CLASS ALLEGATIONS

68. Plaintiff brings this action as a class action on his own behalf and on behalf of all other persons similarly situated as members of the proposed Class and Subclass, under CR 23(a) and (b)3.

69. The proposed Class is defined as:

> All persons residing in the United States whose personally identifiable information Kaye-Smith obtained, stored and/or shared and which was exposed to an unauthorized party as the result of the data breach referenced in BECU's correspondence to Plaintiff Smith dated July 25, 2022.

Plaintiff reserves the right to modify, change, or expand the Class definition, including proposing subclasses, based on discovery and further investigation.

70. Excluded from the Class are Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendants have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

71. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of his claims on a class-wide basis using the same evidence that would be used to prove those elements in individual actions alleging the same claims.

72. Numerosity and Ascertainability. The members of the Class are so numerous that a joinder of all members would be impracticable. Kaye-Smith holds itself out as a leading Northwest marketing execution and supply chain company, serving corporate clients across a wide range of industries. BECU, in turn, is the largest credit union in the state of Washington with more than 1.16 million members. The PII of over 344,000 BECU members was compromised during Kaye-Smith's Data Breach and thus the Class contains at least that many members. The Class Members are readily ascertainable from information and records in the possession, custody, or control of Kaye-Smith. Notice of this action can readily be provided to the Class.

73. Commonality and Predominance (CR 23(a)(2) and CR 23(b)(3)). There are numerous questions of law and fact common to Plaintiff and members of the Class. Those common questions of law or fact predominate over questions that may affect only individual Class members. The common issues arising from Kaye-Smith's conduct predominate over any individual issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy. The questions of law and fact common to Plaintiff and members of the Class include, among others, the following:

a. Whether and to what extent Defendant had a duty to protect the PII of Plaintiff and Class Members;

b. Whether Defendant failed to adequately safeguard the PII of Plaintiff and Class Members;

c. When Defendant actually learned of the Data Breach;

d. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;

e. Whether Defendant failed to implement and maintain sufficient security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

f. Whether Defendant adequately addressed and ensured that the vulnerabilities that permitted the Data Breach to occur had been fixed;

g. Whether Plaintiff and the Class were intended third party beneficiaries of the contract between Kaye-Smith and BECU.

h. Whether Kaye-Smith breached implied duties to the Class Members that were created by its contract with BECU.

i. Whether Plaintiff and Class Members are entitled to damages as a result of Defendant's wrongful conduct; and

j. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and ongoing harm faced because of the Data Breach.

74. Typicality. Plaintiff's claims are typical of the claims of all Class Members in that the PII of the representative Plaintiff, like that of all Class Members, was compromised in the Data Breach. The evidence and legal theories regarding Kaye-Smith's alleged failings are substantially the same for Plaintiff and all the Class Members.

75. Adequacy. Plaintiff will fairly and adequately protect the interests of the Class. Plaintiff has retained capable and competent attorneys who have significant experience in complex and class action litigation, including consumer rights litigation. Plaintiff and his counsel are committed to prosecuting this action vigorously on behalf of the Class and have the financial

resources to do so. Neither Plaintiff nor his counsel have interests that are contrary to or that conflict with those of the Class.

76. Superiority. Plaintiff and Class Members have suffered and will continue to suffer harm and damages as a result of Defendants' conduct. Absent a class action, most Class members would likely find the cost of litigating their claims prohibitive. Class treatment is superior to multiple individual suits or piecemeal litigation because it conserves judicial resources, promotes consistency and efficiency of adjudication, provides a forum for small claimants, and deters illegal activities. There will be no significant difficulty in the management of this case as a class action.

VI. CHOICE OF LAW

77. This action arises from a Data Breach of PII that BECU collected from Plaintiff and each Class Member at branches located in the State of Washington. It further arises from the performance of a contract that was created and performed in the State of Washington and from the safeguarding of PII that was transferred to Defendant from computer servers located in Washington and, on information and belief, was stored in Washington.

78. Under applicable conflicts of laws principles regarding both common law contracts and torts, the substantive law of the state of Washington governs the claims in this action.

VII. CLAIMS

First Cause of Action

Negligence

79. Plaintiff incorporates the above allegations as if fully set forth here.

80. As a condition of being members of BECU, BECU's current and former members were obligated to provide BECU with certain PII.

81. In the course of providing vendor services as part of its business and for its own profit, Kaye-Smith obtained and accepted possession of the PII of Plaintiff and Class Members

including their names, Social Security numbers, bank account numbers, home addresses, phone numbers, and dates of birth

82. Kaye-Smith has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Subclass could and would suffer if the PII were wrongfully disclosed. Kaye-Smith knew or should have known that Plaintiff's and Class' sensitive PII was an attractive target to cyber thieves.

83. Kaye-Smith knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII of Plaintiff and the Class involved an unreasonable risk of harm to Plaintiff and the Class, even if the harm occurred through the criminal acts of a third party. Kaye-Smith uniquely knows the importance of protecting PII from cyber criminals.

84. Kaye-Smith had a non-delegable duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing both its security protocols to ensure that the PII of Plaintiff and the Class that was in its possession was adequately secured and protected.

85. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

86. Plaintiff and the Class and Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendants knew or should have known of the inherent risks in collecting, storing, and sharing the PII of Plaintiff and the Class and Class, along with the critical importance of ensuring adequate security of that PII at all times.

87. Defendant had the ability to sufficiently guard against data breaches. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and the Class. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect the PII of Plaintiff and the Class in the face of increased risk of theft.

88. Defendant breached the duty to exercise reasonable care in protecting Plaintiff's and the Class Members' PII by failing to take reasonable security measures, and by ensuring that its vendors took reasonable security measures, to safeguard and adequately secure the PII of Plaintiff and the Class Members from unauthorized access.

89. Under RCW 19.255.010(1), Kaye-Smith also owed a duty to timely disclose to Plaintiff and to the Class Members that their PII had been, or was reasonably believed to have been, compromised. Timely disclosure was necessary so that Plaintiff and the Class members could, among other things: (1) purchase identity protection, monitoring, and recovery services; (2) flag asset, credit, and tax accounts for fraud, including by reporting the theft of their social security numbers to financial institutions, credit agencies, and the IRS; (3) purchase or otherwise obtain credit reports; (4) place or renew fraud alerts on a quarterly basis; (5) routinely monitor loan data and public records; and (6) take other steps to protect themselves and recover from identity theft.

90. Kaye-Smith breached its duty to timely disclose the Data Breach to Plaintiff and the Class Members. After learning of the Data Breach, Kaye-Smith unnecessarily delayed notifying Plaintiff and Class Members in a sufficiently conspicuous manner.

91. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Class, the PII of Plaintiff and the Class would not have been compromised.

92. There is a causal connection between Defendants' failure to implement and/or maintain security measures to protect the PII of Plaintiff and the Class and the harm, or risk of

imminent harm, suffered by Plaintiff and the Class. The PII of Plaintiff and the Class was lost and accessed as the proximate result of Defendants' failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

93. As a direct and proximate result of Defendant's failings, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity to control how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake adequate measures to protect the PII of Plaintiff and the Class; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Class.

94. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and the Class suffered and will suffer the continued risks of exposure of their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

Second Cause of Action

Breach of Implied Contract

95. Plaintiff incorporates the above allegations as if fully set forth here.

96. BECU required Plaintiff and Class Members to provide their personal information, including names, Social Security numbers, home addresses, phone numbers, dates of birth, and other personal information, as a condition of being customers (or members) of BECU, which Plaintiff and each Class Member provided.

97. BECU and Kaye-Smith contracted for services for which Plaintiff and the Class were the intended beneficiaries, and under which Kaye-Smith has undertaken duties to act for the benefit of Plaintiffs and the Class.

98. As part of its contractual performance, Kaye-Smith accepted possession of the PII of Plaintiff and the Class and agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class Members if their data had been breached and compromised or stolen.

99. Kaye-Smith breached the contractual duties it undertook for the benefit of Plaintiff and the Class by failing to safeguard and protect their personal and financial information and by failing to provide timely and accurate notice to them that personal and financial information was compromised as a result of the Data Breach.

100. As a direct and proximate result of Kaye-Smith's above-described breach, Plaintiff and the Class have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

Third Cause of Action

Invasion of Privacy

101. Plaintiff incorporates the above allegations as if fully set forth here.

102. Plaintiff and the Class members reasonably expected that the sensitive personal information entrusted to BECU would be kept private and secure, including by vendors who contracted with BECU, and would not be disclosed to any unauthorized third party or for any improper purpose.

103. Kaye-Smith unlawfully invaded the privacy rights of Plaintiff and Class Members by:

a. failing to adequately secure their sensitive personal information from disclosure to unauthorized third parties or for improper purposes;

b. enabling the disclosure of personal and sensitive facts about them in a manner highly offensive to a reasonable person; and

c. enabling the disclosure of personal and sensitive facts about them without their informed, voluntary, affirmative, and clear consent.

104. A reasonable person would find it highly offensive that Kaye-Smith, having accepting Plaintiff's and the Class members' sensitive personal information, failed reasonably to protect that information from unauthorized disclosure to third parties.

105. In failing to adequately protect Plaintiff's and the Class members' sensitive personal information, Kaye-Smith acted in reckless disregard of their privacy rights. Kaye-Smith knew or should have known that its ineffective security measures, and the foreseeable consequences thereof, are highly offensive to a reasonable person in Plaintiff's and the Class members' position.

106. Kaye-Smith violated Plaintiff's and the Class members' right to privacy under the common law.

107. Kaye-Smith's unlawful invasions of privacy damaged Plaintiff and the Class members. As a direct and proximate result of Kaye-Smith's unlawful invasions of privacy, Plaintiff and the Class members suffered significant anxiety and distress, and their reasonable expectations of privacy were frustrated and defeated. Plaintiff and the Class Members seek actual and nominal damages for these invasions of privacy.

Fourth Cause of Action

Washington Consumer Protection Act

RCW 19.86, *et seq*.

108. Plaintiff incorporates the above allegations as if fully set forth here.

109. Kaye-Smith is a person within the meaning of the Washington Consumer Protection Act, RCW 19.86.010 and it conducts "trade" and "commerce" within the meaning of RCW 19.86.010(2).

110. Plaintiff and the Class members are "persons" within the meaning of RCW 19.86.010(1).

111. Kaye-Smith engaged in unfair or deceptive acts or practices in the conduct of its business by the conduct set forth above. These unfair or deceptive acts or practices include: failing to adequately secure Plaintiff's and the Class members' sensitive personal information from disclosure to unauthorized third parties or for improper purposes; enabling the disclosure of personal and sensitive facts about Plaintiff and the Class members in a manner highly offensive to a reasonable person; enabling the disclosure of personal and sensitive facts about Plaintiff and the Class members without their informed, voluntary, affirmative, and clear consent; and omitting,

suppressing, and concealing the material fact that Defendant did not reasonably or adequately secure Plaintiff's and the Class members' sensitive personal information.

112. Kaye-Smith's systematic acts or practices are unfair because they (1) caused substantial financial injury to Plaintiff and the Class members; (2) are not outweighed by any countervailing benefits to consumers or competitors; and (3) are not reasonably avoidable by consumers.

113. Kaye-Smith's systematic acts or practices are unfair because the acts or practices are immoral, unethical, oppressive, and/or unscrupulous.

114. Kaye-Smith's systematic acts deceptive as they were and are capable of deceiving a substantial portion of the public.

115. Kaye-Smith's unfair or deceptive acts or practices have repeatedly occurred in trade or commerce within the meaning of RCW 19.86.010 and RCW 19.86.020 and are ongoing and/or have a substantial likelihood of being repeated.

116. Kaye-Smith's unfair or deceptive acts or practices impact the public interest.

117. As a direct and proximate result of Kaye-Smith's unfair or deceptive acts or practices, Plaintiff and the Class members have suffered injury in fact.

118. As a result of Kaye-Smith's conduct, Plaintiff and the Class members have suffered actual damages including from fraud and identity theft, time and expenses related to monitoring their financial accounts for fraudulent activity, an increased and imminent risk of fraud and identity theft, the lost value of their personal information, and other economic and non-economic harm.

119. Plaintiff and the Class members are therefore entitled to legal relief against Kaye-Smith's, including recovery of nominal damages, actual damages, treble damages, injunctive relief, attorneys' fees and costs, and such further relief as the Court may deem proper.

120. Plaintiff and the Class members are also entitled to injunctive relief in the form of an order prohibiting Kaye-Smith's from engaging in the alleged misconduct and such other equitable relief as the Court deems appropriate.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for an order:

a. Certifying this case as a class action, appointing Plaintiff as Class representative, and appointing Plaintiff's counsel to represent the Class;

b. Entering judgment for Plaintiff and the Class;

c. Awarding Plaintiff and Class Members monetary relief;

d. Ordering appropriate injunctive relief;

e. Awarding pre and post judgment interest as prescribed by law;

f. Awarding reasonable attorneys' fees and costs as permitted by law; and

g. Granting such further relief as may be just and proper.

Plaintiff further demands trial by jury.

\\\ \\\ \\\

\\\ \\\ \\\

\\\ \\\ \\\

\\\ \\\ \\\

\\\ \\\ \\\

\\\ \\\ \\\

\\\ \\\ \\\

\\\ \\\ \\\

\\\ \\\ \\\

DATED this 6th day of October, 2022.

Respectfully submitted,

s/ Justin M. Baxter
Justin M. Baxter, Oregon State Bar ID Number 992178
Email: justin@baxterlaw.com
BAXTER & BAXTER, LLP
8835 S.W. Canyon Lane, Suite 130
Portland, Oregon 97225
Telephone (503) 297-9031
Facsimile (503) 291-9172

Ari Y. Brown, *subject to application for admission pro hac vice*
Robert Rhodes, *subject to application for admission pro hac vice*
RHODES LEGAL GROUP, PLLC
918 South Horton Street, Suite 901
Seattle, Washington 98134
206-708-7852
Fax 206-906-9230

John Heenan, *subject to application for admission pro hac vice*
Joseph P. Cook, *subject to application for admission pro hac vice*
HEENAN & COOK
Email: john@lawmontana.com
Email: joe@lawmontana.com
1631 Zimmerman Trail
Billings, Montana 59102
Telephone: (406) 839-9081

Attorneys for Plaintiffs